UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/597,003	07/06/2006	Gil Sever	P-9541-US	4617

49443 7590 12/15/2009

Pearl Cohen Zedek Latzer, LLP
1500 Broadway
12th Floor
New York, NY 10036

EXAMINER	
ANDERSON, MICHAEL D	

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
12/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/597,003	**Applicant(s)** SEVER ET AL.
	Examiner MICHAEL ANDERSON	**Art Unit** 2433

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 and all intervening claims (2-20, and 35), are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method including steps of receiving a data portion during communication, processing the data portion, determining if a decision can be reached, and determining whether to allow the data communication is broad enough that the claim could be completely performed mentally, verbally, or without a machine nor is any transformation apparent. For example a person could receive data during communication, process that data, determine if a decision can be reached from review of the data, and determine whether to allow that data communication which would allow the specific data to be processed in respect to the person's needs.

Claim 21 and all intervening claims (22-34) are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to software per se, which does not fall into the categories of “process”, “machine”, “manufacture” and “composition of matter”. Referring to claim 21, claim 21 recites the limitation, “a client agent communicated to a private network”, where par.0012 of Server et al states that the client agent is software module, which directs the claim to software per se .

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-15, and 17-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent Number: 6,134,591 to Nickles, in view of Patent Number: 4,799,153 to Hann et al (hereafter referenced as Hann).

Regarding **claim 1**, Nickles discloses “A method for protecting the transfer of data between a computer and a device” ***(security server protects network resources and information [Abstract/ lines 3-10]),*** “the method comprising the steps of: a.)receiving a data portion during a data communication session”***(utilizing a gateway component, security server prepares program modules to receive data[Col.11/lines 60-63]), “***the data portion being associated with a particular physical communication port of the computer and with the device that is currently communicating via the particular physical communication port", ***i.e. capability to transfer/receive data from port of computer to server(security server communicates with external devices via I/O port[Col.9/lines 1-2];***."b.)processing the data portion according to a protocol that is associated with the physical communication port" ***(Communication protocol allows data to be transferred to physical communication of multiple ports [Col.3/lines 36-40]);*** "c.)determining whether a decision on the data communication session may be reached" ***(network security server issues a general ticket which is used to authenticate access/communication requests Col.2/lines 36-42]),*** Nickles does not explicitly disclose "if not storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for the next data portion, if yes, proceed to step'd'; d.)determining whether to allow the data communication session, if yes transferring the one or more data portions with data that are stored in the associated buffer, if any exist, toward or from the physical communication port, if not modifying the data transportation." However Hann in an analogous art discloses security communication system in which host security device intercepts and processes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal. ***(Hann [Abstract/lines 11-18] also see buffer storage Hann [Co1.11/lines 48-56]).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nickles network security integration method and system with a security communication system in which host security device intercepts and processes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal in order to provide additional security as suggested by Hann***(Hann[Abstract/lines 11-18] also see buffer storage Hann[Co1.11/lines 48-56]).***

Regarding **claim 2**, in view of claim 1, the references combined disclose "wherein the step of modifying the data transportation further comprises blocking the transportation"***(if gateway authentication is satisfied, security server will determine if user of computer system is authorized to access/communicate with object identified in request Nickles[Col.10/ lines 38-43]).***

Regarding **claim 3**, in view of claim 1, the references combined disclose “wherein the step of modifying the data transportation further comprises modifying the type of the transportation”, ***(Common Gateway interface CGI format is translated and transformed to a format accessible by application Nickles[Col.14/lines 44-49]).***

Regarding **claim 4**, in view of claim 1, the references combined disclose “wherein the step of modifying the data transportation further comprises modifying the status of a requested file” (***Common Gateway interface CGI format is translated and transformed to a format accessible by application Nickles[Col.14/lines 44-49]).***

Regarding **claim 5**, in view of claim 1, the references combined disclose “wherein the step of modifying the data transportation further comprises correcting the data according to the communication protocol***"(see debug option Nickles[Col.16/lines21-23***]).

Regarding **claim 6**, in view of claim 1, the references combined disclose "wherein the physical communication port is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared"***(see computer system bus and I/O port interface Nickles[Fig.4/items 84 & 85] also see Nickles[Col.9/lines1-2]).***

Regarding **claim 7**, in view of claim 1, the references combined disclose "wherein the physical communication port is a USB port. ***(see computer system bus and I/O port interface Nickles [Fig.4/items 84 & 85] also see Nickles [Col.9/lines1-2]).*** Regarding **claim 8**, in view of claim 1, the references combined disclose "wherein the physical communication port is wireless" ***(see computer system bus and I/O port interface Nickles [Fig.4/items 84 & 85] also see Nickles [Col.9/lines1-2]).***

Regarding **claim 9**, in view of claim 1, the references combined disclose "wherein the step of processing the data portion further comprising: (i) determining whether additional processing based on a higher level protocol is required, and if not continuing at step 'c', otherwise continue at step (ii); and (ii) processing part of the data portion that is relevant to the higher level protocol according to the higher level protocol and returning to step (i)., ***i.e. utilizing data tables, security system makes decision to send request of additional authentication (object manager program module performs specific tasks based on information received from security server Nickles [Col.10/ lines62- Col.11/ line 7] also see Object manager Nickles [Fig.6/***

item 20]).

Regarding **claim 10**, in view of claim 9, the references combined disclose "wherein the step of processing part of the data portion further comprises processing relevant to a higher level protocol that is associated with the device" ***i.e. utilizing data tables, security system makes decision to send request of additional authentication (object manager program module performs specific tasks based on information received from security server Nickles[Col.10/ lines62- Col.11/ line 7] also see Object manager Nickles[Fig.6/ item 20])***

Regarding **claim 11**, in view of claim 10, the references combined disclose "wherein the device is an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols" ***(see computer system bus and I/O port interface Nickles [Fig.4/items 84 & 85] also see Nickles [Col.9/lines1-2]).***

Regarding **claim 12**, in view of claim 1, the references combined disclose "wherein the step of processing the data portion is performed in respect of the data that is stored in the associated buffer" ***(host security device intercepts and process initial data packet information containing user authorization information which is stored from buffer Hann [Abstract/lines 11-18] see buffer storage Hann [Co1.11/lines 48-56]).***

Regarding **claim 13**, in view of claim 1, the references combined disclose "wherein the step of determining whether a decision on the data communication session may be reached, is performed in respect of the data that is stored in the associated buffer" ***(host security device intercepts and process initial data packet information containing user authorization information which is stored from buffer Hann [Abstract/lines 11-18] see buffer storage Hann [Co1.11/lines 48-56]).***

Regarding **claim 14**, in view of claim 1, the references combined disclose "wherein the step of determining whether a decision to allow the data communication session is performed in respect of the data that is stored in the associated buffer" ***(host security device intercepts and process initial data packet information containing user authorization information which is stored from buffer Hann [Abstract/lines 11-18] see buffer storage Hann [Co1.11/lines 48-56]).***

Regarding **claim 15**, in view of claim 1, the references combined disclose "wherein the step of receiving a data portion further comprises receiving a data portion that is selected from a group consisting of packet and SCSI block." ***(host security device intercepts and process initial data packet information containing user authorization information Hann [Abstract/lines 11-18].***

Regarding **claim 17**, in view of claim 1, the references combined disclose "wherein step of receiving the data portion further comprises obtaining the data portion by emulating a filter module", ***i.e. duplicating the functions of filtering/receiving text information from client computer (computer program module receives data information from source/client computer system Nickles[Col.3/lines 52-63]).***

Regarding **claim 18**, in view of claim 1, the references combined disclose "wherein the step of processing the data portion according to a protocol that is associated with the physical communication port further comprises: parsing the data portion, reassembling the data; and analyzing the reassembled data" ***i.e. analyzing data and determining next process(object manager program module performs specific tasks based on information received from security server Nickles[Col.10/ lines62- Col.11/ line 7] also see Object manager Nickles[Fig.6/ item 20]).***

Regarding **claim 19**, in view of claim 1, the references combined disclose "wherein the step of determining whether to allow the communication session further comprises reviewing the security policy"***(security server reviews transaction table database information Nickles[Col.12/lines 15-26]).***

Regarding **claim 20**, in view of claim 1, the references combined disclose "wherein the step of determining whether to allow the communication session further comprises examining the working environment in which the computer is operating and only allowing the communication for certain working environments" ***(security server reviews transaction table database information which contains different scenarios and options the server can utilize Nickles [Col.12/lines 15-26]).***

Regarding **claim 21**, Nickles discloses "A system for enhancing the security of a private network being accessed by a computer" ***(security server protects network resources and information [Abstract/ lines 3-10]),*** "the system comprising:
a client agent that is communicatively coupled to the private network and is associated with a computer operating on the private network"***(see Client agent[Fig.1/item 16] connected to network[Fig.1/item14] which interconnects with a security server allowing connection to private network [Fig.1/item12])*** , "the client agent having an

associated security policy; a security manager that is communicatively coupled to the private network; the client agent being operative to: detect a data transfer passing between a device connected to the computer through a physical communication port of the computer" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize Nickles[Col.12/lines 15-26]).*** ; "and verify the data transfer is allowable based on the analysis of the data and the security policy; and the security manager being operable to associate a security policy with the client agent" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize Nickles[Col.12/lines 15-26]),*** Nickles does not explicitly disclose "analyze the data transfer according to the communication protocol associated with the physical communication port." However Hann in an analogous art discloses security communication system in which host security device intercepts and processes/analyzes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal. ***(Hann [Abstract/lines 11-18] also see buffer storage Hann [Co1.11/lines 48-56]).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nickles network security integration method and system with a security communication system in which host security device intercepts and processes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal in order to provide additional security as suggested by Hann***(Hann[Abstract/lines 11-18] also see buffer storage Hann[Co1.11/lines 48-56]).***

Regarding **claim 22**, in view of claim 21, the references combined disclose "wherein the security manager is operable to verify that the security policy is correct" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize when verifying Nickles[Col.12/lines 15-26]).***

Regarding **claim 23**, in view of claim 21, the references combined disclose "wherein the security policy includes a plurality of rules that at least define limits on data transfers during a communication session" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios, rules and options the server can utilize when verifying Nickles [Col.12/lines 15-26]).***

Regarding **claim 24**, in view of claim 21, the references combined disclose "wherein the security policy includes a plurality of rules that at least define the type of operations that can be performed during a communication session" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios, rules and options the server can utilize when verifying Nickles [Col.12/lines 15-26]).***

Regarding **claim 25**, in view of claim 21, the references combined disclose "wherein the security manager is operable to disable any communication with the computer unless the client agent associated with the computer is active" ***(Nickles[Fig.12B/item 1232 user's transaction is aborted if password is invalid also see Nickles[Col.19/ lines 50-54]).***

Regarding **claim 26**, in view of claim 21, the references combined disclose "wherein the physical communication ports can be selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared" ***(see computer system bus and I/O port interface Nickles[Fig.4/items 84 & 85] also see Nickles[Col.9/lines1-2]).***

Regarding **claim 27**, in view of claim 21, the references combined disclose "wherein the physical communication ports are a USB port" ***(see computer system bus and I/O port interface Nickles [Fig.4/items 84 & 85] also see Nickles [Col.9/lines1-2]).***

Regarding **claim 28**, in view of claim 21, the references combined disclose "wherein the physical communication ports is wireless" ***(see computer system bus and I/O port interface Nickles [Fig.4/items 84 & 85] also see Nickles [Col.9/lines1-2]).***

Regarding **claim 29**, in view of claim 21, the references combined disclose "wherein the client agent is associated with the security policy by loading the security policy into the client agent" ***(within tables used by object manager is contained a user table which specifies which users have access and works with an associated network protocol loaded on clients computer such as HTTP, FTP, e-***

mail and TELNET Nickles [Col.13/lines 60-67] also see user tables Nickles [Col.12/ lines26-30]).

Regarding **claim 30**, in view of claim 21, the references combined disclose "wherein the security manager is operable to verify that the security policy loaded into the client agent has not been modified" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios, rules and options the server can utilize when verifying Nickles [Col.12/lines 15-26]).***

Regarding **claim 31**, in view of claim 21, the references combined disclose "wherein the client agent is further operative to transmit a report to the security server, the report identifying events that occurred with the computer in view of the security policy"***(client computer transmits log data to security server specifying where to log data of systems [Col.15/lines 9-22]).***

Regarding **claim 32**, in view of claim 21, the references combined disclose "wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with a device selected from a group consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle"***(authorization functions are performed in conjunction with tables which specify the different levels of authorization [Col.6/lines 7-16], each device or computer connected to network is assigned a unique code which corresponds to table[Col.7/ lines20-21]).***

Regarding **claim 33**, in view of claim 21, the references combined disclose “wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols” ***(authorization functions are performed in conjunction with tables which specify the different levels of authorization [Col.6/lines 7-16], each device or computer connected to network is assigned a unique code which corresponds to table [Col.7/ lines20-21]).***

Regarding **claim 34,** (original) A software agent installed in a computer for enhancing the security of the computer” ***(security server protects network resources and information [Abstract/ lines 3-10])***, “the agent being operative to:
detect a data transfer passing through at least one physical communication port of the computer” ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize Nickles[Col.12/lines 15-26])***; “and verify the data transfer is allowable based on the analysis of the data and a security policy” ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize Nickles[Col.12/lines 15-26])***
Nickles does not explicitly disclose “ analyze the data transfer according to the communication protocol associated with the at least one physical communication port” However Hann in an analogous art discloses security communication system in which host security device intercepts and processes/analyzes initial data packet information

which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal.***(Hann[Abstract/lines 11-18] also see buffer storage Hann[Co1.11/lines 48-56]).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nickles network security integration method and system with a security communication system in which host security device intercepts and processes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal in order to provide additional security as suggested by Hann***(Hann[Abstract/lines 11-18] also see buffer storage Hann[Co1.11/lines 48-56]).***

Regarding **claim 35**, in view of claim 10, the references combined disclose "wherein the device is a device selected from a group of devices consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle" ***(see client computer system Nickles [Fig.1/item 16] which contains a hard disc drive, floppy, CD ROM).***

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Patent Number: 6,134,591 to Nickles, in view of Patent Number: 4,799,153 to Hann et al (hereafter referenced as Hann), in further view of Patent Number: US 6,769,071 to Cheng et al (hereafter referenced as Cheng).

Regarding **claim 16**, in view of claim1, Nickles and Hann do not explicitly disclose "wherein the step of receiving the data portion further comprises obtaining the data portion by emulating a class driver." However Cheng in an analogous art discloses a class driver designed to operate storage devices being used in conjunction with a computer storage system ***Cheng [Col.5/ lines19-24].***

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nickles network security integration method and Hann's security communication system in which host security device intercepts and processes initial data packet information with a class driver designed to operate storage devices being used in conjunction with a computer storage system in order to provide the additional feature of operating a large number of different devices of broadly similar types as suggested by Cheng ***Cheng[Col.5/ lines19-24].***

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

He et al (Patent Number.: 6,088,451) discloses a security system and method for network element access.

Apte et al (Patent No.: US 6,467,040 B1) discloses a client authentication by server not known at request time.

Eschelbeck et al (Patent No.: US 6,611,869 B1) discloses a system and method for providing trustworthy network security concern communication in an active security management environment.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL ANDERSON whose telephone number is (571)270-5159. The examiner can normally be reached on Monday-Friday 8am til 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2433

MICHAEL ANDERSON
Examiner, Art Unit 2433